UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

In re LastPass Data Security Incident Litigation	Case No.: 1:22-cv-12047-PBS
JASON BECKERMAN, ROBERT LEE, REDA ELAMRI, SETH ARNOFF, MIRON LULIC, JUSTIN COOKE, and JEFFREY LEWIS, Plaintiffs, v. **LASTPASS US LP**, Defendant.	Case No. 1:24-cv-10874-PBS Judge Patti B. Saris **JURY TRIAL DEMANDED**

SECOND AMENDED COMPLAINT

Plaintiffs Jason Beckerman, Robert Lee, Reda Elamri, Seth Arnoff, Miron Lulic, Justin Cooke, and Jeffrey Lewis ("Plaintiffs") bring this action ("Complaint") against Defendant LastPass US LP ("LastPass" or "Defendant") and allege upon information and belief, except as to their own actions, the investigation of counsel, and the facts that are a matter of public record, as follows:

NATURE OF THE ACTION

1. LastPass provides "a password manager tool" to its customers "that allows users to store, secure, and autofill their passwords."[1] Essentially, the password manager tool allows

[1] https://www.lastpass.com/why-lastpass

users the ability to use a single and supposedly secure master password to access password protected accounts across the internet, *e.g.*, banking, email, or social media accounts. LastPass represents the password manager tool to its customers as an "auto-pilot for all your passwords" giving its users "peace of mind everywhere you go."[2]

2. In addition to the password manager tool, "LastPass users get a password vault, which is the encrypted part of the LastPass password manager where a user's passwords, secure notes, and sensitive information are safely stored."[3] LastPass represents to customers that the secure vaults ("LastPass Vault") are "like a physical safe but for your online valuables."[4] Indeed, LastPass represents to current and prospective users that they can safely secure confidential and sensitive information like credit card and payment information, secure credentials for accessing websites and digital applications, and even Social Security numbers and driver's license information in their LastPass Vault.[5]

3. LastPass touts the security of its service and the LastPass Vaults throughout its website and marketing materials. LastPass ensures users that their LastPass Vaults can only be accessed through the user's secure master password and that "[d]ata stored in your vault is kept secret, even from LastPass." Moreover, LastPass repeatedly ensures its users that "Your Security Is Our Top Priority" and that "LastPass uses industry-standard encryption and hashing with salting so that you, and only you, can login to your vault."

4. Unfortunately for Plaintiffs who relied on these and other representations when deciding whether to store sensitive confidential and financial information in their LastPass

[2] Password management from anywhere, https://www.lastpass.com
[3] *Id.*
[4] Password Vault Software, https://www.lastpass.com/features/password-vault
[5] *Id.*

Vaults, between August 8 and August 12 of 2022, an unauthorized party was able to compromise a LastPass engineer's corporate laptop and use the access credentials to exfiltrate LastPass source code, technical information, and certain LastPass internal system secrets (the "Data Breach").[6]

5. Subsequently, between August 12 and August 26 of 2022, the attackers used information acquired in the initial attack to target and compromise the computer of a LastPass Senior Development Engineer. During this period, "the threat actor copied information from backup that contained basic customer account information and related metadata including company names, end-user names, billing addresses, email addresses, telephone numbers, and the IP addresses from which customers were accessing the LastPass service."[7] This information, including end-user names and other identifying information was unencrypted and fully accessible to the threat actors at the time of the Data Breach.[8]

6. Most importantly, the attackers acquired backup copies of the customer LastPass Vault database. This database, which LastPass reassured users remained encrypted and inaccessible, contained all the sensitive and confidential information that Plaintiffs and millions of other LastPass customers stored in their supposedly secure LastPass Vaults at the time it was acquired by the threat actors.

---

[6] Incident 1 – Additional details of the attack, https://support.lastpass.com/s/document-item?language=en_US&bundleId=lastpass&topicId=LastPass/incident-1-details.html&_LANG=enus

[7] Notice of Recent Security Incident, https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/

[8] https://support.lastpass.com/s/document-item?language=en_US&sfdcIFrameOrigin=null&bundleId=lastpass&topicId=LastPass/incident-data.html&_LANG=enus

7. Despite this valuable information being in the hands of cybercriminals, Defendant waited until November 30, 2022 to inform Plaintiffs that certain customer information had been acquired in the Data Breach and until December 22, 2022 to inform its users that a copy of their LastPass Vaults had been exfiltrated and acquired during the Data Breach. After the November disclosure, LastPass promised Plaintiffs that "LastPass products and services remain fully functional"[9] and following the December disclosure, LastPass promised amongst, other representations, that:

> **it would take millions of years to guess your master password using generally-available password-cracking technology. Your sensitive vault data, such as usernames and passwords, secure notes, attachments, and form-fill fields, remain safely encrypted based on LastPass' Zero Knowledge architecture. There are no recommended actions that you need to take at this time.[10]**

8. Defendant continues to represent that Plaintiffs need to only ensure that their master password complies with LastPass's recommendations and denies that LastPass secure vaults are vulnerable to access. However, because the attackers were able to exfiltrate a backup copy of the LastPass Vault, they can use off the shelf and commercially available hardware to brute force millions of password guesses per second. Moreover, because the exfiltrated customer LastPass Vault backup is offline, none of the standard brute force defenses, *i.e.*, locking accounts after a certain number of failed password attempts or alerting users to attempts to access their accounts, would have prevented access to information that Plaintiffs stored in their customer LastPass Vaults at the time the backup data base was exfiltrated.

9. Plaintiffs read and relied on LastPass's representations and assurances to their detriment. LastPass knew or could not have been unaware at the time Plaintiffs decided to use

[9] *Id.*
[10] *Id.*, emphasis in original

the LastPass platform that its data security protocols were below industry standards and that its organizational, administrative, and technical safeguards were insufficient to protect against the known and foreseeable risk of a targeted cyberattack. LastPass knew or was reckless in not knowing and in failing to warn that information stored in LastPass Vaults prior to August 26, 2022 was vulnerable to access. On information and belief, LastPass concealed or disregarded risks to Plaintiffs of which it was or should have been aware. LastPass's willful failure to warn was calculated to prevent damage to LastPass's image as a secure information storage platform in an effort to retain users and continue to attract users to its service. LastPass knowingly and willfully made partial representations that omitted material information and failed to correct prior representations when it learned of their falsity or inaccuracy.

10. As a result of these misrepresentations and omissions, Plaintiffs each subsequently discovered that the private keys to their cryptocurrency wallets that they stored only in their LastPass Vaults and took great measures to protect from unauthorized access or disclosure, had been accessed and used to move their digital assets to wallets controlled by an unknown third party.

11. The theft of Plaintiffs' digital assets was the direct result of LastPass's willful and knowing failure to warn them that information stored in their LastPass Vaults could be accessed by criminals who perpetrated a breach of LastPass's network beginning in August of 2022.

PARTIES

12. Plaintiff Jason Beckerman is a citizen and resident of Delray Beach, Florida.

13. Plaintiff Robert Lee is a citizen and resident of Buffalo Grove, Illinois.

14. Plaintiff Reda Elamri is a citizen and resident of Kansas City, Missouri.

15. Plaintiff Seth Arnoff is a citizen and resident of Yorkville, Illinois.

16. Plaintiff Miron Lulic is a citizen and resident of North Tustin, California.

17. Plaintiff Justin Cooke is a citizen and resident of Spring Texas.

18. Plaintiff Jeffrey Lewis is a citizen and resident of Mountain View California.

19. Defendant LastPass US LP is a limited partnership organized under the laws of Delaware and with its principal place of business located in Boston, Massachusetts.

20. The acts or omissions giving rise to Plaintiffs' claims all were conceived of, directed from, and emanated from Defendant's Boston headquarters.

JURISDICTION AND VENUE

21. This Court has subject matter jurisdiction under 28 U.S.C. § 1332 as all Plaintiffs are residents of separate states from Defendant and the amount in controversy exceeds the sum of $75,000.

22. This Court has general personal jurisdiction over Defendant because it maintains its principal place of business in this District, regularly conducts business in Massachusetts, and has sufficient minimum contacts in Massachusetts.

23. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District

FACTUAL ALLEGATIONS

Defendant's Business

24. Defendant operates a cloud based secure information storage platform and holds itself out as protecting its users "with pervasive security protection" and "[b]est-in-class encryption," while boasting of its"[g]lobal security certifications." LastPass serves millions of

consumers across the world and provides secure storage solutions and other IT services for over 100,000 global business.[11]

25. As part of its consumer facing business, LastPass offers a universal password manager that allows a user to access password protected accounts across websites with a single master password.[12] LastPass also offers the LastPass Vault that it represents is secure enough to store the most sensitive personal information including credit card and payment information, access credentials and even Social Security numbers and driver's license information. [13]

26. LastPass promises prospective and current users that it complies with applicable laws and industry standards regarding data security and that it employes appropriate organizational, administrative, and technical safeguards.

27. LastPass represents that information stored in the LastPass vaults is accessible only to the users and that "it would take millions of years" to brute force a master password.[14]

28. Plaintiffs are former users of LastPass who used the LastPass Vault to store their confidential financial information and read and relied on Defendant's representations that information stored on the LastPass Vault was secure from unauthorized access.

29. Prior to the Data Breach, LastPass assured users that "LastPass is designed to keep sensitive data safe using a local-only security model: And that its encryption algorithm "is widely accepted as impenetrable – it's the same encryption type utilized by banks and the military."[15] However, unbeknownst to Plaintiffs at the time they chose to use the LastPass Vaults,

---

[11] https://www.lastpass.com/
[12] https://www.lastpass.com/why-lastpass
[13] *Id.*
[14] https://bgr.com/tech/last-years-lastpass-security-breach-was-linked-to-35-million-in-crypto-heists/
[15] https://web.archive.org/web/20220809215337/https://www.lastpass.com/security/zero-knowledge-security, as of August 9, 2022

Defendant's encryption practices were substandard and failed to comply with the industry standard 310,000 password count iterations.

30. And following the Data Breach, Plaintiffs specifically chose to continue using the service based on LastPass's representations concerning the integrity of the information stored in LastPass Vaults. From August 25 of 2022 to the time that Plaintiffs assets were stolen. LastPass repeatedly reassured Plaintiffs that their information was secure so long as their master passwords were configured according to LastPass's recommendations. However, LastPass did not force users to implement certain standards when creating a password prior to August 26, 2022 nor did it require users to upgrade old passwords. In fact, LastPass did not affirmatively require users to update or replace their master password since at least 2018. Accordingly, a user that configured their LastPass password based on previous guidance would not have known or suspected that their LastPass vault was vulnerable to a brute force attack at the time the customer vault backup was stolen.

31. In reliance on the representations referenced herein, and others, Plaintiffs stored the private keys to their digital asset wallets, which they used to store their digital assets and, in some cases, interact with decentralized finance protocols, on their LastPass Vaults.

32. Despite these precautions, each Plaintiff discovered that, subsequent to the August 2022 data breach, the private keys that they stored only in their LastPass Vaults had been accessed and used to move their assets to wallets controlled by an unknown third party.

33. The theft of Plaintiffs' assets was the direct result of LastPass's willful and knowing failure to warn them that their data security protocols were substandard prior to the Data Breach and that information stored in their LastPass Vaults could be accessed by criminals who perpetrated a breach of LastPass's network beginning in August of 2022. Defendant failed

to warn Plaintiffs that information stored in their LastPass Vaults was vulnerable in order to protect its reputation as provider of secure information storage solutions and to continue to derive revenue from new and existing users.

The Data Breach and Defendant's False Assurances to Plaintiffs

34. On August 12, 2022 LastPass detected anomalous activity on its network and determined that an unauthorized actor had acquired certain information. On or about August 25, 2022, LastPass began notifying users of the platform by email that "an unauthorized party gained access to portions of the LastPass development environment" but assured users that there was "no evidence that this incident involved any access to customer data or encrypted password vaults."

35. However, between August 12 and August 26 of 2022, the attackers used information acquired in the initial attack to compromise the home computer of a Senior Developer and one of only four individuals with access to the backup user vault database. Once they were able to access the cloud environment on which the database was stored, the attacker exfiltrated it and gained access to all sensitive user information stored thereon, albeit encrypted.

36. LastPass further warranted to its users, including Plaintiffs, that "[LastPass's] products and services are operating normally."

37. LastPass further advised that information stored in LastPass Vaults was neither compromised nor at risk and that "we don't recommend any action on behalf of our users or administrators" in response to the Data Breach.

38. On September 15, 2022, LastPass again advised its users that their information was secure and assured them that "We can also confirm that there is no evidence that this incident involved any access to customer data or encrypted password vaults." LastPass assured

users that "our system design and controls prevented the threat actor from accessing any customer data or encrypted password vaults."

39. Additionally, LastPass warranted that information stored in LastPass vaults was safe because "without the master password, it is not possible for anyone other than the owner of a vault to decrypt vault data as part of our Zero Knowledge security model."

40. On November 30, 2022, LastPass acknowledged that despite the implementation of additional security and containment measures, the attackers were subsequently "able to gain access to certain elements of our customers' information" but LastPass still reassured users that their data was secure because "customers' passwords remain safely encrypted due to LastPass's Zero Knowledge architecture."

41. LastPass did not advise its users to remove sensitive information from their Vaults or to monitor the information stored thereon for instances of misuse or unauthorized access. Rather, LastPass again promised that "we can confirm that LastPass products and services remain fully functional," and only warned users to "follow our best practices around setup and configuration of LastPass," none of which, though already followed by Plaintiffs, would have prevented the access to or misuse of the information stored on their LastPass Vaults at the time of the data breach.

42. On December 22, 2022, LastPass finally acknowledged that unauthorized actors did access and exfiltrate a backup copy of customer vault data but again reassured users that their data was safely encrypted:

> The threat actor was also able to copy a backup of customer vault data from the encrypted storage container which is stored in a proprietary binary format that contains both unencrypted data, such as website URLs, as well as fully-encrypted sensitive fields such as website usernames and passwords, secure notes, and form-filled data. **These encrypted fields remain secured with 256-bit AES encryption and can only be decrypted with a unique encryption key derived from each user's master password using our Zero**

> **Knowledge architecture. As a reminder, the master password is never known to LastPass and is not stored or maintained by LastPass.** The encryption and decryption of data is performed only on the local LastPass client. (emphasis in the original)

43. LastPass further assured users that any information stored on their LastPass Vaults was securely encrypted and safe from unauthorized access and that they need take no action to protect the stored data so long as their master password had not been compromised, "**Your sensitive vault data, such as usernames and passwords, secure notes, attachments, and form-fill fields, remain safely encrypted based on LastPass' Zero Knowledge architecture. There are no recommended actions that you need to take at this time**." (Emphasis in the original).

44. On March 1, 2023 LastPass published a final update regarding the data breach to its users in which it discussed in detail the timeline of the data breach and the nature of the information compromised. Again, LastPass assured users that:

> All sensitive customer vault data, other than URLs, file paths to installed LastPass Windows or macOS software, and certain use cases involving email addresses, were encrypted using our Zero knowledge model and can only be decrypted with a unique encryption key derived from each user's master password.

45. As before, LastPass did not instruct Plaintiffs to monitor or secure the assets stored on their LastPass Vaults at the time the customer vault data was exfiltrated or to take any action aside from ensuring that their master passwords were securely configured and safe from compromise.

46. Indeed, in the Security Bulletin: Recommended Actions for Free, Premium, and Families Customers[16] published by LastPass on March 1, 2023, LastPass only recommended

[16] *Security Bulletin: Recommended Actions for Free, Premium, and Families Customers*, March 1, 2023, available at, https://support.lastpass.com/s/document-item?language=en_US&bundleId=lastpass&topicId=LastPass/security-bulletin-recommended-actions-free-premium-families.html&_LANG=enus

that users securely configure their passwords and use multi-factor authentication on their accounts. However, none of these measures would have prevented the unauthorized access to information stored on Plaintiffs' LastPass Vaults because changing a password or implementing multi-factor authentication would not affect the attackers' attempts to access the *offline* backup copy of customer LastPass Vaults.

47. Plaintiffs each read and relied on LastPass's representations concerning the integrity of their LastPass Vaults following the data breach and understood that, because their master passwords were configured according to LastPass's recommendations, they need not take any preventive measures in response to the data breach. They understood from LastPass that it would have taken "**millions of years to guess [their] master password using generally-available password-cracking technology**." (emphasis in the original).

48. As a result, Plaintiffs continued to rely on their LastPass Vaults as the sole, and what they believed to be the safest, location to store their private keys. Plaintiffs followed LastPass's guidance regarding configuring their master passwords and did not recycle or reuse previous passwords.

49. The only means of access to Plaintiffs' private keys was through their LastPass Vaults which were secured using master passwords and not shared with others.

50. Importantly, LastPass guidance regarding passwords was misleading because changing the master password or implementing multi-factor authentication would not prevent access to information stored in LastPass Vaults before August 26, 2022. Because the attackers acquired a backup copy that is essentially frozen in time and inaccessible to outside manipulation, they are free to brute force the passwords using millions of guesses per second. "[W]hen cybercrooks can get their hands on the encrypted vault data itself — as opposed to

having to interact with LastPass via its website[,] "offline" attacks allow the bad guys to conduct unlimited and unfettered "brute force" password cracking attempts against the encrypted data using powerful computers that can each try millions of password guesses per second."[17] In essence the attackers are free to work with a database of user information that exists as it did at the time it was exfiltrated and without security concerns slowing down or preventing their brute force attacks.

51. LastPass uses a version of Password-Based Key Derivation Function ("PBKDF2") to encrypt passwords. PBKDF2 works, in part, by hashing or scrambling the password for a set number of times to create a master encryption key. The number of times that a password is hashed is called the iteration count and the higher the number, the greater the security of the resulting encryption key. A password iteration count of 5,000 for example, means that the password is hashed 5,000 times to create a decryption key. At the time of the Data Breach the industry standard for PBKDF2 was 310,000 iterations.[18]

52. In 2018, after being warned that LastPass' password iteration count of 5,000 was below industry standards,[19] LastPass began updating its users' password iterations to 100,100, meaning that each master password is hashed 100,100 times to create a master encryption key. Inexplicably however, LastPass failed to update the password iteration count for many of its users, and following the Data Breach, users discovered that their password iteration counts were as low as 5,000, or in some cases as low as 1.[20][21] As one security researcher noted:

---

[17] *Experts Fear Crooks are Cracking Keys Stolen in LastPass Breach*, Sept. 5, 2023, available at, https://krebsonsecurity.com/2023/09/experts-fear-crooks-are-cracking-keys-stolen-in-lastpass-breach/

[18] https://palant.info/2022/12/28/lastpass-breach-the-significance-of-these-password-iterations/

[19] https://palant.info/2022/12/28/lastpass-breach-the-significance-of-these-password-iterations/

[20] https://twit.tv/posts/transcripts/security-now-episode-905-transcript

[21] https://palant.info/2022/12/28/lastpass-breach-the-significance-of-these-password-iterations/

> The password iterations setting hasn't been updated for existing accounts, leaving some accounts configured with 1 iteration despite the default being 100,100 since 2018. My test account in particular is configured with 5,000 iterations which, quite frankly, shouldn't even be a valid setting.[22]

53. Other security researchers examining the Data Breach noted that:

> LastPass somehow failed to update those iteration counts for a decade after the default was raised from 1 to 500 in June of 2012. And they have not immediately and proactively assumed responsibility for that by informing their users, whose iteration counts were dangerously low, in many cases set to 1, that unfortunately, they should now assume that the unencrypted content of their LastPass vaults is now in the hands of criminals.[23]

54. Moreover, LastPass does not appear to have updated the default password iteration count of 100,100 since 2018, despite the industry standard at the time of the Data Breach requiring at least a 310,000 iteration count to protect against unauthorized decryption.[24]

55. Accordingly, Defendant's representations that it would take millions of years to brute force access to a LastPass Vault following the Data Breach were false and misleading at the time they were made. Even a password with 50 bits of entropy (i.e., an unusually strong password) would take only one year to crack using a 200-GPU password cracking rig and "[a] typical strength password that's been protected by 100,100 iterations of key derivation, that's attacked by a 200-GPU password cracking rig would fall against that attack in an average of 71.338 days."[25] And for accounts protected with only a 1, 500, or 5,000 iteration count, that time is reduced to mere minutes. The equipment to assemble a machine capable of brute forcing access to a LastPass vault can be easily built using commercially available hardware.[26]

---

[22] https://palant.info/2023/02/28/lastpass-breach-update-the-few-additional-bits-of-information/
[23] https://www.grc.com/sn/SN-905-Notes.pdf at p. 6
[24] https://palant.info/2022/12/28/lastpass-breach-the-significance-of-these-password-iterations/
[25] https://www.grc.com/sn/SN-905-Notes.pdf at p. 6
[26] *Id.*

56. LastPass also stored users' Vault metadata in plain text, meaning it was intelligible to anyone with access to it. The unencrypted metadata allows anyone to associate company names, end user names, physical addresses, email addresses, telephone numbers, and IP addresses with specific Vaults.[27] Additionally, the unencrypted metadata includes "the deobfuscated URL that's associated with the website's encrypted logon record. Taken as a whole these are all of the sites for which LastPass's vault contained your logon information."[28]

57. Crucially here, LastPass's failure to encrypt metadata allowed the attackers to selectively focus their efforts on brute forcing passwords to user Vaults that they know will have sensitive information. "[A]ssuming that it's possible for the bad guys to associate company names, end user names, physical addresses, eMail addresses, telephone numbers and IP addresses with specific vaults, the result – without any decryption – is a comprehensive dump of 'exactly who logs on exactly where'"[29]

58. These vulnerabilities were well known to Defendant for years prior to the Data Breach. As far back as 2015, security researchers warned LastPass that unencrypted Vault metadata was accessible and that ECB encryption, used by LastPass to obfuscate certain password information, leaked information concerning password length and other characteristics.[3031] In 2017, security researchers warned LastPass that URLs of websites visited by the Vault owner were accessible and insufficiently obfuscated[32] and in 2018, LastPass was warned that its password iteration count was well below industry standards.[33] Despite updating

[27] https://twit.tv/posts/transcripts/security-now-episode-905-transcript
[28] https://www.grc.com/sn/SN-905-Notes.pdf at p. 4
[29] https://www.grc.com/sn/SN-905-Notes.pdf at p. 4
[30] https://www.blackhat.com/docs/eu-15/materials/eu-15-Vigo-Even-The-Lastpass-Will-Be-Stolen-deal-with-it.pdf at p. 67
[31] https://www.grc.com/sn/SN-905-Notes.pdf at p. 5
[32] https://hackernoon.com/psa-lastpass-does-not-encrypt-everything-in-your-vault-8722d69b2032
[33] https://palant.info/2018/07/09/is-your-lastpass-data-really-safe-in-the-encrypted-online-vault/#the-encrypted-vault-myth

the setting for new accounts in 2018, LastPass failed to update the password iteration count for existing users and failed to update to iteration counts to industry standards at the time of the Data Breach in 2022.

59. LastPass also failed to implement reasonable and industry standard remote access protocols for its employees. The Data Breach resulted from a LastPass engineer accessing highly sensitive company data from a compromised home computer. Had Defendant restricted or monitored remote access activity it would have prevented or detected the Data Breach sooner. Moreover, LastPass failed to properly monitor its network activity and should have had systems in place to detect and prevent the transfer of large volumes of data, particularly sensitive data, from its systems. Defendant's failure to implement reasonable and industry standard monitoring and to limit remote access to sensitive data allowed criminals unfettered access for fourteen days, from August 12, 2022 to August 26, 2022. LastPass was aware of these vulnerabilities and failed to remedy or disclose them to Plaintiffs. Defendant obfuscated and hid these material facts from Plaintiffs both at the time they began using the service and the time following the Data Breach.

60. LastPass was well aware of the potential for access to users' LastPass Vaults as least as early as November 2023 when it acknowledged that user data was exfiltrated in the Data Breach and presumably knew that its Senior Developer's access credentials had been used to exfiltrate the user vault database. Accordingly, LastPass could not have been unaware that actions user's took to update their passwords or protect their accounts would have no impact or effect on the exfiltrated customer LastPass Vault backup.

61. Moreover, LastPass users both publicly posted through Twitter and elsewhere, and on information and belief reported directly to LastPass that, despite strict security precautions, their digital assets had been drained from their wallets following the Data Breach.

62. And, security researchers also publicly linked the theft of digital assets from users' of LastPass and detailed the methodology that they used to conclude that private keys were acquired through the data breach.[34] Of note, security researchers reliably linked "the theft of more than $35 million in crypto from more than 150 confirmed victims, with roughly two to five high-dollar heists happening each month since December 2022."

63. The researchers further noted that victims of the LastPass Vault vulnerability were:

> longtime cryptocurrency investors, and security-minded individuals [and] [i]mportantly, none appeared to have suffered the sorts of attacks that typically preface a high-dollar crypto heist, such as the compromise of one's email and/or mobile phone accounts… The victim profile remains the most striking thing, they truly all are reasonably secure. They are also deeply integrated into this ecosystem, [including] employees of reputable crypto orgs, VCs, people who built DeFi protocols, deploy contracts, run full nodes.[35]

64. The researchers also posted an analysis showing the flow of assets stolen using private keys stored on LastPass and noted the unique signature of the digital asset thefts.[36]

65. This information was shared with LastPass prior to its publication on September 5, 2023, and LastPass knew of the connection between the compromise of private keys and the

[34] *Experts Fear Crooks are Cracking Keys Stolen in LastPass Breach*, Sept. 5, 2023, available at, https://krebsonsecurity.com/2023/09/experts-fear-crooks-are-cracking-keys-stolen-in-lastpass-breach/
[35] *Id.*
[36] *Id.*

LastPass platform but nevertheless knowingly and willfully failed to correct their earlier statements.[37]

66. Despite being aware of this information, LastPass failed to warn Plaintiffs that their private keys, or any other sensitive information stored in their LastPass Vaults was vulnerable to compromise as a result of the data breach.

67. Defendant had a duty to notify Plaintiffs that they were aware of reports of access to information stored in LastPass Vaults and warn them to remove sensitive information from their LastPass Vaults. Nonetheless, Defendant failed to provide Plaintiffs with such notification.

68. LastPass knew that its representations concerning the integrity of information stored on customer Vaults were misleading, inaccurate, and insufficient to protect Plaintiffs from the misuse of the data that they stored in their LastPass Vaults.

69. LastPass knew prior to the compromise of Plaintiffs' LastPass Vaults that its representations concerning the integrity of information stored on customer Vaults were misleading, inaccurate, and insufficient to protect Plaintiffs from the misuse of the data that they stored in their LastPass Vaults.

70. LastPass knew at the time Plaintiffs began using the service that its representations regarding the safety and security of its LastPass Vaults were false and misleading and that its internal security practices were below industry standards and insufficient to protect against the foreseeable threat of a targeted cyberattack.

71. LastPass knew that the representations in its terms of service regarding compliance with industry standards and its implementation of "organizational, administrative,

[37] *Id.*

and technical safeguards" was substandard and insufficient to safeguard information stored in LastPass Vaults.

72. LastPass's failure to properly secure and safeguard its platform from unauthorized access to and exfiltration of user data, its failure to properly investigate and disclose its findings regarding the data breach and the security of user information, and its failure to warn and to correct earlier representations regarding the security of user information were conducted willfully and knowingly and constitute unfair and deceptive acts and practices in violation of Mass Gen. Ch. 93A.

73. Defendant disregarded the rights of Plaintiffs by knowingly, intentionally, willfully, or recklessly failing to properly investigate and identify vulnerabilities to information stored in users' LastPass Vaults following the access to and exfiltration of the back copies of the LastPass Vault database between August 12 and August 26 of 2022. Defendant omitted material information from its disclosures regarding the Data Breach and misrepresented that LastPass Vaults remained secure. Defendant was under a continuing duty to correct partial or ambiguous statements and to disclose facts material to the security and integrity of the LastPass Vaults.

74. Defendant's failure to disclose material facts and to warn Plaintiffs that their confidential information was vulnerable to unauthorized access was done knowingly and willfully and done to protect the brand image of LastPass and to retain current users while enticing new users to the service.

75. Had LastPass warned users that their accounts were vulnerable to access, rather than assuring them that they need take no action in response to the data breach, Plaintiffs would

have transferred their digital assets to unique wallets with new private keys and prevented the theft of their digital assets from private keys stored in their LastPass vaults.

76. As a result of Defendant's failure to secure its systems, failure to implement expected industry standard data security protocols, failure to reasonably investigate the consequences of the Data Breach and failure to warn Plaintiffs that their confidential information was vulnerable to access following discovery that the backup database of the LastPass Vaults had been exfiltrated was the direct and proximate cause of Plaintiffs' injuries as alleged herein.

PLAINTIFFS' EXPERIENCES

Plaintiff Jason Beckerman

77. Plaintiff Beckerman is a LastPass user who used Defendant's LastPass Vault to store his confidential information, including the private key to his digital asset wallet. Plaintiff Beckerman paid a fee in exchange for access to LastPass's services, including his LastPass Vault.

78. Plaintiff Beckerman read and relied on Defendant's representations concerning the security of information stored in the LastPass Vault and read and relied on Defendant's representations concerning the integrity and sufficiency of Defendant's data security protocols. Due to the confidential nature of the information he stored in his LastPass Vault, Plaintiff Beckerman would not have used Defendant's services had Defendant disclosed the true state of its data security practices.

79. Plaintiff Beckerman is well experienced in the world of digital assets and followed strict security practices with respect to storing and maintaining the confidentiality of his private keys. Plaintiff Beckerman has not shared or disclosed his private keys to anyone and the LastPass Vault is the only internet accessible or digital environment on which he stored his private keys.

Plaintiff Beckerman only interacted with trusted protocols and always verified the legitimacy of links or applications that he accessed with his wallets.

80. Plaintiff Beckerman read and relied on LastPass's representations concerning the integrity of their LastPass Vaults following the Data Breach and understood that, because his master password was securely configured, he need not take any preventive measures in response to the Data Breach.

81. Despite Plaintiff Beckerman's security precautions, on October 25, 2023, Plaintiff Beckerman discovered that the private key to his Ethereum wallet, stored only in his LastPass Vault, was used to access his wallet, unwind his leveraged positions in decentralized protocols, and to transfer 523.14 Ethereum to a wallet controlled by an unknown third party. The theft of Plaintiff Beckerman's assets was the direct result of LastPass's willful and knowing failure to warn him that information stored in his LastPass Vault could be accessed by.

82. Plaintiff Beckerman suffered actual injury from having his private key to his digital asset wallet compromised as a result of the Data Breach including the loss of 523.14 Ethereum from his digital asset wallet and the loss of profits resulting from the forced unwinding of his leveraged positions of 2,885 Ethereum at the time his assets were stolen. The present day value of that position is approximately $9,200,000.

Plaintiff Robert Lee

83. Plaintiff Lee is a LastPass user who used Defendant's LastPass Vault to store his confidential information, including the private keys to his digital asset wallet. Plaintiff Lee paid a fee in exchange for access to LastPass's services, including his LastPass Vault.

84. Plaintiff Lee read and relied on Defendant's representations concerning the security of information stored in the LastPass Vault and read and relied on Defendant's

representations concerning the integrity and sufficiency of Defendant's data security protocols. Due to the confidential nature of the information he stored in his LastPass Vault, Plaintiff Lee would not have used Defendant's services had Defendant disclosed the true state of its data security practices.

85. Plaintiff Lee is well experienced in the world of digital assets and followed strict security practices with respect to storing and maintaining the confidentiality of his private keys. Plaintiff Lee has not shared or disclosed his private keys to anyone and the LastPass Vault is the only internet accessible or digital environment on which he stored his private keys. Plaintiff Lee only interacted with trusted protocols and always verified the legitimacy of links or applications that he accessed with his wallets.

86. Plaintiff Lee read and relied on LastPass's representations concerning the integrity of their LastPass Vaults following the Data Breach and understood that, because his master password was securely configured, he need not take any preventive measures in response to the Data Breach.

87. Despite Defendant's assurances, following the Data Breach, Plaintiff Lee discovered that the private keys that he stored only in his LastPass Vault had been accessed and used to move 152.35 Ethereum, 0.026 Bitcoin, and 9,577.09 Golem from his digital asset wallet to wallets controlled by an unknown third party.

88. Had LastPass warned him that the information stored on his LastPass Vault was vulnerable to access, he would have transferred his digital assets to a new wallet with a secure private key and prevented the loss of his assets.

89. Plaintiff Lee suffered actual losses from having his private key to his digital asset wallet compromised as a result of the Data Breach including the loss of 152.35 Ethereum, 0.026 Bitcoin, and 9,577.09 Golem from his digital asset wallet.

Plaintiff Reda Elamri

90. Plaintiff Elamri is a LastPass user who used Defendant's LastPass Vault to store his confidential information, including the private keys to his digital asset wallet. Plaintiff Elamri paid a fee in exchange for access to LastPass's services, including his LastPass Vault.

91. Plaintiff Elamri read and relied on Defendant's representations concerning the security of information stored in the LastPass Vault and read and relied on Defendant's representations concerning the integrity and sufficiency of Defendant's data security protocols. Due to the confidential nature of the information he stored in his LastPass Vault, Plaintiff Elamri would not have used Defendant's services had Defendant disclosed the true state of its data security practices.

92. Plaintiff Elamri is well experienced in the world of digital assets and followed strict security practices with respect to storing and maintaining the confidentiality of his private keys. Plaintiff Elamri has not shared or disclosed his private keys to anyone and the LastPass Vault is the only internet accessible or digital environment on which he stored his private keys. Plaintiff Elamri only interacted with trusted protocols and always verified the legitimacy of links or applications that he accessed with his wallets.

93. Plaintiff Elamri read and relied on LastPass's representations concerning the integrity of their LastPass Vaults following the Data Breach and understood that, because his master password was securely configured, he need not take any preventive measures in response to the Data Breach.

94. Despite Defendant's assurances, following the Data Breach, Plaintiff Elamri discovered that the private keys that he stored only in his LastPass Vault had been accessed and used to move 45.104 Ethereum and certain Non-Fungible Tokens from his digital asset wallet to wallets controlled by an unknown third party.

95. Had LastPass warned him that the information stored on his LastPass Vault was vulnerable to access, he would have transferred his digital assets to a new wallet with a secure private key and prevented the loss of his assets.

96. Plaintiff Elamri suffered actual losses from having his private key to his digital asset wallet compromised as a result of the Data Breach including the loss of 45.104 Ethereum from his digital asset wallets and the fair market value of the Non-Fungible Tokens that he stored in his digital asset wallet.

Plaintiff Seth Arnoff

97. Plaintiff Arnoff is a LastPass user who used Defendant's LastPass Vault to store his confidential information, including the private keys to his digital asset wallet. Plaintiff Arnoff used the free version of LastPass's services, including his LastPass Vault.

98. Plaintiff Arnoff read and relied on Defendant's representations concerning the security of information stored in the LastPass Vault and read and relied on Defendant's representations concerning the integrity and sufficiency of Defendant's data security protocols. Due to the confidential nature of the information he stored in his LastPass Vault, Plaintiff Arnoff would not have used Defendant's services had Defendant disclosed the true state of its data security practices.

99. Plaintiff Arnoff is well experienced in the world of digital assets and followed strict security practices with respect to storing and maintaining the confidentiality of his private

keys. Plaintiff Arnoff has not shared or disclosed his private keys to anyone and the LastPass Vault is the only internet accessible or digital environment on which he stored his private keys. Plaintiff Arnoff only interacted with trusted protocols and always verified the legitimacy of links or applications that he accessed with his wallets.

100. Plaintiff Arnoff read and relied on LastPass's representations concerning the integrity of their LastPass Vaults following the Data Breach and understood that, because his master password was securely configured, he need not take any preventive measures in response to the Data Breach.

101. Despite Defendant's assurances, following the Data Breach, Plaintiff Arnoff discovered that the private keys that he stored only in his LastPass Vault had been accessed and used to move 12,700.27 Tomb, 597,009.5 Retreeb, 15,153,436 Zookeeper, 0.0044 Deus Finance, 0.524 Stader, 0.00863 Ethereum, 8.374 LiquidDriver, 90.54 BeethovenX, and 9.054 Equalizer Dex tokens from his digital asset wallet to wallets controlled by an unknown third party.

102. Had LastPass warned him that the information stored on his LastPass Vault was vulnerable to access, he would have transferred his digital assets to a new wallet with a secure private key and prevented the loss of his assets.

103. Plaintiff Arnoff suffered actual losses from having his private key to his digital asset wallet compromised as a result of the Data Breach including the loss of 12,700.27 Tomb, 597,009.5 Retreeb, 15,153,436 Zookeeper, 0.0044 Deus Finance, 0.524 Stader, 0.00863 Ethereum, 8.374 LiquidDriver, 90.54 BeethovenX, and 9.054 Equalizer Dex tokens from his digital asset wallet.

Plaintiff Miron Lulic

104. Plaintiff Lulic is a LastPass user who used Defendant's LastPass Vault to store his confidential information, including the private keys to his digital asset wallet. Plaintiff Lulic paid a fee in exchange for access to LastPass's services, including his LastPass Vault.

105. Plaintiff Lulic read and relied on Defendant's representations concerning the security of information stored in the LastPass Vault and read and relied on Defendant's representations concerning the integrity and sufficiency of Defendant's data security protocols. Due to the confidential nature of the information he stored in his LastPass Vault, Plaintiff Lulic would not have used Defendant's services had Defendant disclosed the true state of its data security practices.

106. Plaintiff Lulic is well experienced in the world of digital assets and followed strict security practices with respect to storing and maintaining the confidentiality of his private keys. Plaintiff Lulic has not shared or disclosed his private keys to anyone and the LastPass Vault is the only internet accessible or digital environment on which he stored his private keys. Plaintiff Lulic only interacted with trusted protocols and always verified the legitimacy of links or applications that he accessed with his wallets.

107. Plaintiff Lulic read and relied on LastPass's representations concerning the integrity of their LastPass Vaults following the Data Breach and understood that, because his master password was securely configured, he need not take any preventive measures in response to the Data Breach.

108. Despite Defendant's assurances, following the Data Breach, Plaintiff Lulic discovered that the private keys that he stored only in his LastPass Vault had been accessed and used to move 1.29026194 Bitcoin, 14.5 Ethereum, 30.446087 Chainlink, 98.1 Solana, 507.33

USDC, and 6,458.78 TrueUSD from his digital asset wallet to wallets controlled by an unknown third party.

109. Had LastPass warned him that the information stored on his LastPass Vault was vulnerable to access, he would have transferred his digital assets to a new wallet with a secure private key and prevented the loss of his assets.

110. Plaintiff Lulic suffered actual losses from having his private keys to his digital asset wallet compromised as a result of the Data Breach including the loss of 1.29026194 Bitcoin, 14.5 Ethereum, 30.446087 Chainlink, 98.1 Solana, 507.33 USDC, and 6,458.78 TrueUSD from his digital asset wallets.

Plaintiff Justin Cooke

111. Plaintiff Cooke is a LastPass user who used Defendant's LastPass Vault to store his confidential information, including the private keys to his digital asset wallet. Plaintiff Cooke paid a fee in exchange for access to LastPass's services, including his LastPass Vault.

112. Plaintiff Cooke read and relied on Defendant's representations concerning the security of information stored in the LastPass Vault and read and relied on Defendant's representations concerning the integrity and sufficiency of Defendant's data security protocols. Due to the confidential nature of the information he stored in his LastPass Vault, Plaintiff Cooke would not have used Defendant's services had Defendant disclosed the true state of its data security practices.

113. Plaintiff Cooke is well experienced in the world of digital assets and followed strict security practices with respect to storing and maintaining the confidentiality of his private keys. Plaintiff Cooke has not shared or disclosed his private keys to anyone and the LastPass Vault is the only internet accessible or digital environment on which he stored his private keys.

Plaintiff Cooke only interacted with trusted protocols and always verified the legitimacy of links or applications that he accessed with his wallets.

114. Plaintiff Cooke read and relied on LastPass's representations concerning the integrity of their LastPass Vaults following the Data Breach and understood that, because his master password was securely configured, he need not take any preventive measures in response to the Data Breach.

115. Despite Defendant's assurances, following the Data Breach, Plaintiff Cooke discovered that the private keys that he stored only in his LastPass Vault had been accessed and used to move 8.14700107 Bitcoin, and 24.68 Ethereum from his digital asset wallet to wallets controlled by an unknown third party.

116. Had LastPass warned him that the information stored on his LastPass Vault was vulnerable to access, he would have transferred his digital assets to a new wallet with a secure private key and prevented the loss of his assets.

117. Plaintiff Cooke suffered actual losses from having his private keys to his digital asset wallet compromised as a result of the Data Breach including the loss of 8.14700107 Bitcoin, and 24.68 Ethereum from his digital asset wallets.

Plaintiff Jeffrey Lewis

118. Plaintiff Lewis is a LastPass user who used Defendant's LastPass Vault to store his confidential information, including the private keys to his digital asset wallets. Plaintiff Lewis paid an annual fee in exchange for access to LastPass's services, including his LastPass Vault.

119. Plaintiff Lewis read and relied on Defendant's representations concerning the security of information stored in the LastPass Vault and read and relied on Defendant's representations concerning the integrity and sufficiency of Defendant's data security protocols.

Due to the confidential nature of the information he stored in his LastPass Vault, Plaintiff Lewis would not have used Defendant's services had Defendant disclosed the true state of its data security practices.

120. Plaintiff Lewis is well experienced in the world of digital assets and followed strict security practices with respect to storing and maintaining the confidentiality of his private keys. Plaintiff Lewis has not shared or disclosed his private keys to anyone and the LastPass Vault is the only internet accessible or digital environment on which he stored his private keys. Plaintiff Lewis only interacted with trusted protocols and always verified the legitimacy of links or applications that he accessed with his wallets.

121. Plaintiff Lewis read and relied on LastPass's representations concerning the integrity of their LastPass Vaults following the Data Breach and understood that, because his master password was securely configured, he need not take any preventive measures in response to the Data Breach.

122. Despite Defendant's assurances, following the Data Breach, Plaintiff Lewis discovered that the private keys that he stored only in his LastPass Vault had been accessed and used to transfer his digital assets to wallets controlled by an unknown third party, resulting in losses of 2 Bitcoin, 344.43 Ethereum, 9,515.83 Avalanche Tokens, 63.14 Binance Tokens, and 12.68 Aave.

123. Had LastPass warned him that the information stored on his LastPass Vault was vulnerable to access, he would have transferred his digital assets to a new wallet with a secure private key and prevented the loss of his assets.

124. Plaintiff Lewis suffered actual losses from having his private keys to his digital asset wallet compromised as a result of the Data Breach, including the loss of 2 Bitcoin, 344.43 Ethereum, 9,515.83 Avalanche Tokens, 63.14 Binance Tokens, and 12.68 Aave.

FIRST COUNT
Breach of Contract
(On Behalf of Plaintiffs Beckerman, Lee, Elamri, Lulic, Cooke, and Lewis)

125. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

126. Plaintiffs Beckerman, Lee, Elamri, Lulic, Cooke, and Lewis ("Plaintiffs" for the purposes of this Count) entered into contracts with Defendant under which Plaintiffs paid Defendant in exchange for Defendant's provision of a secure storage environment for sensitive and confidential data.

127. In exchange for payment, Defendant agreed to implement reasonable and industry standard data security to protect Plaintiffs' information against the foreseeable threat of unauthorized access, including through a targeted cyberattack. Defendant further agreed to and to timely and adequately notify them if their information was susceptible to unauthorized access.

128. Specifically, Defendant represented and agreed that:

a. We have implemented and maintain appropriate organizational, administrative, and technical safeguards designed to protect your Content against any unauthorized access, loss, misuse, or disclosure. We also maintain a compliance program that includes independent third-party audits and certifications;[38]

[38] https://web.archive.org/web/20220809171810/https://www.lastpass.com/legal-center/terms-of-service/personal, as of August 9, 2022

b. We maintain a global data privacy program, designed to safeguard and responsibly handle your Content and any associated personal data we may collect and/or process on your behalf;[39]

c. LastPass' technical and organizational security measures are designed to prevent the unauthorized access to personal data, and to ensure the ongoing confidentiality, integrity and availability of LastPass' products and services.[40]

d. LastPass is dedicated to monitoring and continuously improving our security, technical and organizational measures to better protect your sensitive Customer Content. We constantly evaluate industry standard practices regarding technical data privacy and information security and strive to meet or exceed those standards. Our security programs are comprehensive and dedicated to all facets of security.[41]

e. Security is our mission at LastPass. At every step, we've designed LastPass to protect what you store, so you can trust it with your sensitive data. Our password management system protects customer data through powerful security features. We implement strong encryption algorithms and safeguard your account across all devices.[42]

[39] *Id*.
[40] https://web.archive.org/web/20220812175504/https://www.lastpass.com/trust-center/privacy, as of August 12, 2024
[41] https://web.archive.org/web/20220812190940/https://www.lastpass.com/trust-center, as of August 12, 2022
[42] *Id*.

129. Defendant breached its obligation under the contracts it made with Plaintiffs by failing to implement reasonable and industry standard data protection and failing to sufficient administrative, technical, and hardware practices to protect against the foreseeable threat of a cyberattack.

130. Defendant's obligations concerning data security were material to Plaintiffs as that is the core service for which they entered into contracts with Defendant and the core service provided by Defendant, to protect confidential and sensitive information.

131. Plaintiffs performed all of their obligations under the contracts they made with Defendant and suffered from the theft of their digital assets as a result of Defendant's breach of its contractual obligations.

132. As a result of Defendant's breach of its contracts with Plaintiffs, Plaintiffs have been injured as described herein and are entitled to damages available by law, in an amount to be proven at trial.

SECOND COUNT
Breach of Implied Contract
(On Behalf of all Plaintiffs)

133. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

134. Plaintiffs agreed to use Defendant's service, including its LastPass Vaults based on Defendant's representations that it would adequately secure the information in their LastPass Vaults from unauthorized access and that it would implement reasonable and industry standard data security protections.

135. Defendant solicited, offered, and Plaintiffs to store sensitive and confidential information in their LastPass Vaults as part of Defendant's regular business practices. Plaintiffs

accepted Defendant's offers and used the LastPass Vaults as intended and represented by Defendant.

136. Defendant accepted possession of Plaintiffs' sensitive information and entered into implied contracts under which it agreed to and Plaintiffs understood that it would implement reasonable and industry standard data security and timely and adequately notify Plaintiffs of any deficiencies in its security standards or practices or threats to information stored on Defendant's platform.

137. Plaintiffs would not have entrusted their confidential information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

138. Plaintiffs would not have entrusted their confidential information to Defendant in the absence of an implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

139. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

140. Defendant breached the implied contracts it made with Plaintiffs by failing to safeguard and protect their confidential information, by failing to monitor their systems for unauthorized access and unusual activity, by failing to implement reasonable encryption standards and by failing to provide accurate information regarding the security of their LastPass Vaults following the Data Breach.

141. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices, by failing to monitor their systems for unauthorized access and unusual activity, by failing to implement reasonable

encryption standards, and by failing to provide accurate information regarding the security of their LastPass Vaults following the Data Breach.

142. As a result of Defendant's breach of its implied contracts with Plaintiffs, Plaintiffs have been injured as described herein and are entitled to damages available by law, in an amount to be proven at trial.

THIRD COUNT
Violation of Mass. Gen. Laws Ann. 93A, § 1, *et seq.*
(On Behalf of all Plaintiffs)

143. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

144. Defendant and Plaintiffs are "persons" as meant by Mass. Gen. Laws. Ann. Ch. 93A, § 1(a).

145. Defendant operates in "trade or commerce" as meant by Mass. Gen. Laws Ann. Ch. 93A, § 1(b).

146. Defendant advertised, offered, or sold goods or services in Massachusetts and engaged in trade or commerce directly or indirectly affecting the people of Massachusetts, as defined by Mass. Gen. Laws Ann. Ch. 93A, § 1(b).

147. Plaintiffs, through Counsel, sent written demands for relief on behalf of themselves pursuant to Mass. Gen. Laws Ann. Ch. 93A § 9(3). Defendant responded to the 93A letters and denied liability in its response and offered an inadequate remedy (one year of credit monitoring) to Plaintiffs' demand.

148. Based on the allegations above, *supra,* Defendant engaged in unfair methods of competition and unfair and deceptive acts and practices in the conduct of trade or commerce, in violation of Mass. Gen. Laws Ann. Ch. 93A, § 2(a), including, *inter alia*, by:

a. Failing to implement appropriate organizational, administrative, and technical safeguards, failing to implement industry standard password iteration counts, failing to audit their data security practices, failing to update existing account password iteration counts, failing to obscure metadata, failing to limit remote access to sensitive company data, and failing to monitor its systems for the existence of unauthorized access and/or unusual activity;

b. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' confidential information including by failing to prevent or warn of the exfiltration of the customer LastPass Vault backup, leading to the unauthorized access to Plaintiffs' private keys to their digital asset wallets, which was a direct and proximate cause of the Data Breach;

c. Failing to implement industry standard encryption protocols, standards regarding the obfuscation of data, standards governing remote access to sensitive data, and standards regarding the implementation of monitoring practices and threat detection tools;

d. Failing to warn Plaintiffs that information stored in their LastPass Vaults was vulnerable to access and compromise as a result of the access to and exfiltration of the customer LastPass Vault Data Breach in August of 2022;

e. Failing to correct earlier statements regarding the steps that Plaintiffs need to take following the Data Breach and the security and integrity of information that Plaintiffs stored in their LastPass Vaults, which was a direct and proximate cause of the Data Breach;

f. Misrepresenting that re-configuring passwords or implementing multi-factor authentication following the August 2022 exfiltration of the customer LastPass Vault backup would prevent or delay third party attempts to access Plaintiffs' LastPass Vaults;

g. Misrepresenting that LastPass master passwords were practically invulnerable to brute force attacks and that Plaintiffs need take no action following the exfiltration and acquisition of the LastPass Vault backup database in August of 2022;

h. Misrepresenting that prior and/or partial statements regarding the vulnerability of Plaintiffs' LastPass Vaults to unauthorized access remained true despite LastPass's internal investigation and receipt of outside information showing that such statements were inaccurate, false, and/or misleading;

i. Omitting, suppressing, and concealing the material fact that it had received numerically significant reports of access to customer LastPass Vaults following the data breach, including reports of access to securely stored private keys of users' digital asset wallets; and

j. Omitting, suppressing, and concealing the material fact that the only was to ensure that sensitive information stored on LastPass Vaults was protected from compromise was to change non-LastPass credentials associated with that information, or in the case of digital assets, to move those assets into a wallet with a new and secure private key.

149. Each of the Defendant's acts and practices were "unfair" because they fall within the penumbra of common law, statutory, and established concepts of unfairness, given that Defendant solely held the true facts about its inadequate security and the vulnerability of

Plaintiffs' confidential information to third party access, including the private keys to their digital asset wallets, which Plaintiffs could not independently discover.

150. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs, that their confidential information including the private keys to their digital asset wallets were secure and misled Plaintiffs and Class Members into believing they did not need to take actions to secure the information stored in their LastPass Vaults following the data breach.

151. Plaintiffs could not have reasonably avoided injury because the Defendant's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the vulnerability of LastPass vault information to access and theft, Defendant created an asymmetry of information between themselves and consumers that precluded consumers from taking action to avoid or mitigate injury.

152. Defendant's misrepresentations and omissions had no countervailing benefit to consumers or to competition. Defendant intended to mislead Plaintiffs and induce them to rely on its misrepresentations and omissions. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of the Defendant's data security and ability to protect the confidentiality of consumers' confidential information including the private keys to their digital asset wallets.

153. Defendant acted intentionally, knowingly, and maliciously to violate the Massachusetts' Consumer Protection Act, and recklessly disregarded Plaintiffs' rights.

154. As a direct and proximate result of the Defendant's unfair and deceptive trade practices, Plaintiffs have suffered and will continue to suffer injury in the ascertainable losses of

money or property following the theft of their digital assets.

155. Plaintiffs seek all monetary and non-monetary relief allowed by law, including actual damages, double or treble damages, injunctive or other equitable relief, and attorneys' fees and costs.

FOURTH COUNT
Negligent Misrepresentation
(On Behalf of all Plaintiffs)

156. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

157. Defendant represented to Plaintiffs and other users of its platform that it provided a secure platform on which to store sensitive and confidential personal and financial information, that it employed data security standards consistent with applicable laws and industry standards, and that it implemented appropriate organizational, administrative, and technical safeguards to protect information stored in LastPass Vaults.

158. Plaintiffs read and relied on these statements when deciding to store their sensitive personal and financial information in LastPass Vaults.

159. Defendant's representations regarding the security of its platform and the information stored in LastPass vaults was material to Plaintiffs when deciding whether to use Defendant's service and Plaintiffs would not have used LastPass's service had they known that Defendant failed to implement reasonable technical and administrative data security protocols and failed to comply with industry standards.

160. Defendant knew or could not have been unaware of the falsity of its statements regarding the security of information stored in LastPass Vaults as it had been warned by security researchers that its password iteration count was below industry standards, that metadata

associated with LastPass vaults was exposed to unauthorized viewers, that ECB encryption leaked information concerning password characteristics, and other issues identified herein.

161. Defendant knew or could not have been unaware that allowing its developers remote access to highly sensitive information from employees' home computers violated industry standards and allowed for a breach of security by threat actors who could exploit vulnerabilities in those home computers to gain remote access to sensitive information.

162. Defendant had a duty to disclose any inadequacies associated with its data security practices and despite being aware of such inadequacies, Defendant omitted and failed to disclose these material facts to Plaintiffs.

163. Plaintiffs could not have reasonably avoided injury because they reasonably relied on Defendant's misrepresentations concerning the security and integrity of the LastPass platform and Defendant's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from Plaintiffs about the vulnerability of LastPass Vault information to access and theft, Defendant created an asymmetry of information between themselves and consumers that precluded consumers from taking action to avoid or mitigate injury.

164. Moreover, Defendant knew or could not have been unaware that following the Data Breach, Plaintiffs' LastPass Vaults were susceptible to unauthorized access and that its representations to Plaintiffs that they need not take any action to secure the information stored in their LastPass Vaults was false and misleading.

165. Defendant failed to exercise reasonable care in making representations to Plaintiffs concerning the security and integrity of their LastPass Vaults both at the time Plaintiffs decided to use the LastPass platform and following the Data Breach when Plaintiffs were

informed that they need not take action to secure the information stored in their LastPass Vaults.

166. The above-described relationship between Defendant and Plaintiffs is such that, in morals and good conscience, Plaintiffs had the right to rely upon Defendant for accurate information. Defendant was in a special position of confidence and trust with Plaintiffs such that their reliance on Defendant's misrepresentations and omissions was justified.

167. Defendant knew, or reasonably should have known, that Plaintiffs would rely on its misrepresentations and omissions in their decisions regarding whether use the LastPass platform in the first instance and whether to continue to store the private keys to their digital asset wallets on their LastPass Vaults and whether or not they needed to take action to protect themselves and their digital asset wallets from unauthorized access and theft following the Data Breach.

168. Defendant's knowing and willful misrepresentations and omissions regarding the security of LastPass's Vaults, upon which Plaintiffs reasonably and justifiably relied, were intended to induce, and actually induced, Plaintiffs to use the platform and to keep their digital assets stored on LastPass's Vaults.

169. As a direct and proximate cause of their reliance on Defendant's representations, Plaintiffs have been injured as described herein and are entitled to damages available by law, in an amount to be proven at trial.

FIFTH COUNT
Fraudulent Misrepresentation
(On Behalf of all Plaintiffs)

170. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

171. As detailed herein, Defendant's representations regarding steps Plaintiffs needed

to take to protect the confidentiality of the information that they stored on their LastPass Vaults were knowingly and intentionally false, misleading, and omitted information material to Plaintiffs when deciding whether to continue to store sensitive information in their LastPass Vaults following the exfiltration of the customer LastPass Vault backup data base in August of 2022.

172. After learning of information that made its past representations to Plaintiffs inaccurate, misleading, or partially true, Defendant knowingly and willfully failed to correct, update, or clarify those representations.

173. Defendant failed to conduct a reasonable and diligent investigation of the representations they made to Plaintiffs to ensure that those statements were true and that there was no omission of material facts required to make the representations not misleading or false. Defendant, by making partial representations concerning the security and stability of LastPass's Vaults had a duty to fully disclose the risks known to them. Defendant, in the exercise of reasonable care, should have known its statements and omissions were misleading.

174. Defendant misrepresented and failed to correct material facts regarding the integrity of LastPass passwords and the security of information stored on Plaintiffs' LastPass Vaults. These omissions rendered Defendant's affirmative representations deceptive and likely to mislead Plaintiffs.

175. LastPass knew prior to the compromise of Plaintiffs' LastPass Vaults that its representations concerning the integrity of information stored on customer Vaults were misleading, inaccurate, and insufficient to protect Plaintiffs from the misuse of the data that they stored in their LastPass Vaults.

176. Defendant owed a duty to Plaintiffs to speak with care and explain fully and

truthfully all material facts regarding the Data Breach and the security of their LastPass Vaults. Defendant had a duty to correct earlier or partial statements and to disclose the whole truth regarding vulnerabilities to information stored on LastPass Vaults. This duty also arose from statutory bases, including Mass Gen. Ch. 93A and section 5 of the FTC Act, which prohibits "deceptive acts or practices in or affecting commerce." These provisions encompass material representations, omissions, or practices that are likely to mislead reasonable consumers.

177. Defendant's duty to speak with care further arose from the fact that the security of information stored on LastPass vaults is essential to the relationship between Plaintiffs and Defendant and that the security and integrity of information stored on LastPass Vaults was the sole reason that Plaintiffs continued to maintain sensitive information, including the private keys to their digital asset wallets, on their LastPass Vaults following the August 2022 exfiltration of the customer LastPass Vault database backup.

178. The above-described relationship between Defendant and Plaintiffs is such that, in morals and good conscience, Plaintiffs had the right to rely upon Defendant for information. Defendant were in a special position of confidence and trust with Plaintiffs such that their reliance on Defendant's misrepresentations and omissions was justified.

179. Defendant knew, or reasonably should have known, that Plaintiffs would rely on its misrepresentations and omissions in their decisions regarding whether to continue to store the private keys to their digital asset wallets on their LastPass Vaults and whether or not they needed to take action to protect themselves and their digital asset wallets from unauthorized access and theft.

180. Defendant's knowing and willful misrepresentations and omissions regarding the security of LastPass's Vaults, upon which Plaintiffs reasonably and justifiably relied, were

intended to induce, and actually induced, Plaintiffs to keep their digital assets stored on LastPass's Vaults.

181. Defendant made these representations and omissions knowingly and willfully in an attempt to protect the LastPass brand image and to prevent an exodus of users while continuing to entice new users to the LastPass platform.

182. As a direct and proximate cause of their reliance on Defendant's representations, Plaintiffs have been injured as described herein and are entitled to damages available by law, in an amount to be proven at trial.

SIXTH COUNT
Violation of the California Consumer Privacy Act of 2018 ("CCPA")
Cal. Civ. Code § 1798, *et seq.*
(On Behalf of Plaintiffs Lulic and Lewis)

183. Plaintiffs re-allege and incorporate by reference all preceding allegations, as if fully set forth herein.

184. Plaintiffs Lulic and Lewis bring this Count on behalf of themselves ("Plaintiffs" for the purposes of this count).

185. The California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.150(a), creates a private cause of action for violations of the CCPA. Section 1798.150(a) specifically provides:

> Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:
>
> (A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.

(B) Injunctive or declaratory relief.

(C) Any other relief the court deems proper.

186. Defendant is a "business" under § 1798.140(b) in that it is a corporation organized for profit or financial benefit of its shareholders or other owners, with gross revenue in excess of $25 million.

187. Plaintiffs Lulic and Lewis are covered "consumers" under § 1798.140(g) in that they are natural persons who are California residents.

188. The personal information of Plaintiffs Lulic and Lewis at issue in this lawsuit constitutes "personal information" under § 1798.150(a) and 1798.81.5, in that the personal information Defendant collects and which was impacted by the cybersecurity attack includes an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social Security number; (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

189. Specifically, Plaintiffs' unredacted names and other personal identifying information in conjunction with the private keys to their digital asset wallets, which are financial

accounts, were acquired and exfiltrated in the Data Breach as a result of Defendant's failure to implement reasonable data security in violation of the CCPA.

190. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiffs' personal information and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiffs. Specifically, Defendant subjected Plaintiffs' nonencrypted and nonredacted personal information, in combination with financial account information, to an unauthorized access and exfiltration, theft, or disclosure as a result of the Defendant's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

191. As a direct and proximate result of Defendant's violation of its duty, the unauthorized access and exfiltration, theft, or disclosure of Plaintiffs' personal information included exfiltration, theft, or disclosure through Defendant's servers, systems, and website.

192. As a direct and proximate result of Defendant's acts, Plaintiffs were injured and lost money or property as described above.

193. Section 1798.150(b) specifically provides that "[n]o [prefiling] notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages."

194. Accordingly, Plaintiffs Lulic and Lewis by way of this complaint seek actual pecuniary damages suffered as a result of Defendant's violations described herein and all other relief allowed by law.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

A. For an award of actual damages, compensatory damages, double or treble damages, statutory damages, and nominal damages, in an amount to be determined, as allowable by law;

B. For an award of punitive damages, as allowable by law;

C. For an award of attorneys' fees and costs, and any other litigation expenses, including expert witness fees;

D. Pre- and post-judgment interest on any amounts awarded; and

E. Such other and further relief as this court may deem just and proper.

Plaintiffs demand a trial by jury on all claims so triable.

Dated: February 7, 2025

Respectfully submitted,

/s/ John J. Nelson

John J. Nelson (Admitted *Pro Hac Vice)*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
402 W. Broadway, Suite 1760
San Diego, CA 92101
Telephone: (858) 209-6941
Email: jnelson@milberg.com

Randi Kassan
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
100 Garden City Plaza, Suite 500
Garden City, NY 11530
Telephone: (516) 741-5600
Email: rkassan@milberg.com

CERTIFICATE OF SERVICE

I, John J. Nelson, hereby certify that this document was filed on February 7, 2025 through the CM/ECF System and will be served electronically to the registered participants as identified in the Notice of Electronic filing.

/s/ John J. Nelson